

Beschlagnahmung

Nach Beschlagnahmungen geht oft das große Rätselraten los, was wohl potentiell alles für Informationen auf den Geräten gefunden werden könnte. In diesen Momenten fallen uns dann all die kleinen "Sicherheitssünden" ein, die wir so über die Jahre begangen haben: nicht gelöschte Photos, Chats, Kontakte, etc...

Der Schreck sitzt dann oft auch tief und vermischt sich mit der Sorge, was jetzt wohl der Rest der Gruppe sagen wird, wenn sie erfahren, dass sie durch unsere Fehler jetzt eventuell auch Probleme bekommen könnten.

In genau diesen Momenten heißt es dann:

Quote

Warum haben wir uns nicht besser darauf vorbereitet?!

Genau darum geht es in diesem Modul:

Ziele

- Wir wollen hier die Vor- und Nachbereitung einer Beschlagnahmung von technischen Geräten durchspielen.
- Damit wollen wir helfen, mögliche Vorkehrungen zu treffen
- und im Nachhinein die notwendigen Maßnahmen zur Schadensbegrenzung zu ergreifen.

Prävention

Über die folgenden Dinge sollten wir uns im Voraus gut Gedanken machen, da sie uns im Nachhinein viel Stress ersparen können.

Verschlüsselung

- Sind die Geräte verschlüsselt?

- Sind sie mit guten Passwörtern verschlüsselt?
- Sind alle Speichermedien wie USB-Sticks, Festplatten und SD-Karten mit **guten Passwörtern** verschlüsselt?

Passwörter

- Sind alle Passwörter sicher in einem Passwortmanager verwahrt?
 - Gibt es ein aktuelles Backup von der Passwort-Datenbank an einem sicheren Ort?
- Es liegen keine Passwörter auf Papier geschrieben irgendwo herum?
- Habt ihr (*zumindest auf allen wichtigen*) Accounts eine 2-Faktor-Authentifizierung eingerichtet?

Datenhygiene

Je weniger Daten bei euch anfallen, desto weniger Daten können bei euch beschlagnahmt werden:

Lest den Artikel zur Datenhygiene:

Tip

- Wenn Daten anfallen, fragt euch: "Brauchen wir diese Daten wirklich noch?"
- Unverschlüsselte Datenträger im Nachgang spurlos zu verschlüsseln ist nicht unbedingt möglich
- Daten die unverschlüsselt waren können auch nach dem Löschen evtl recovered werden
- verschlüsselte Daten löschen ist kein Problem

Signal

In Signal sollten unbedingt:

- verschwindende Nachrichten eingestellt werden (*zB 1 Woche*), damit eben zu jeder Zeit möglichst wenig Chats auf dem Gerät gespeichert sind.
- das Finden per Telefonnummer deaktiviert werden.
- eine Registrations-PIN gesetzt werden.

Backups

Beschlagnahmung bedeutet: Geräte und Daten weg. Könnt ihr euch möglichst schnell von diesem Verlust "erholen", also eure Daten auf anderen Geräten wieder herstellen?

Backups zu machen ist durchaus nervig, doch ohne Backups kann großer Schaden für euch und andere entstehen. Manchmal zerbrechen langjährige Arbeiten, weil essenzielle Daten/Ergebnisse dieser Arbeit beschlagnahmt wurden und es keine Backup-Strategie gab.

Tip

Deshalb sollten Backups gemacht werden!

Geräte ausschalten

Geräte sind eigentlich nur gut verschlüsselt, wenn sie ausgeschaltet sind, da nach der ersten Entsperrung (direkt nach dem Hochfahren) der Verschlüsselungs-Schlüssel (*en: encryption key*) im Arbeitsspeicher des Gerätes liegt.

Überlegt deshalb, ob ihr in der Situation einer möglichen Beschlagnahmung (Hausdurchsuchung, Demo, Aktion) die Geräte frühzeitig ausmachen könnt.

Tip

- Geräte vor Beschlagnahmung ausschalten!
- Auto Reboot einrichten

Nachbereitung

Nun sind die Geräte beschlagnahmt und außer Reichweite. Sind die oberen Punkte alle beachtet worden? Good Job. Aber was wenn nicht?

Ihr solltet natürlich so oder so möglichst sofort mit einer Anwältin, oder einem Anwalt in Kontakt kommen und von dem Vorgang erzählen. Wir sind keine Jurist*innen und geben daher selbstverständlich keine juristischen Ratschläge. Auch die folgenden Punkte solltet ihr möglichst mit ihnen besprechen.

Evaluation

Failure

Welche Informationen könnten durch diese Beschlagnahme jetzt kompromittiert worden sein?

- Wem solltet/müsst ihr davon berichten?
- Lasst euren Account von Genoss*innen aus sämtlichen Chat-Gruppen entfernen, damit die Behörden nicht mitlesen können.
- ändert möglichst schnell problematische Gruppennamen in Signal. Dabei ist nur sichtbar, **dass** der Name geändert wurde, aber nicht wie die Gruppe vorher hieß. Bei anderen Messengern ist das eventuell nutzlos.
 - *Die letzten beiden Punkte funktionieren natürlich nur, solange das Gerät noch Netzwerkverbindung hat, schadet aber so oder so nicht.*

Failure

Sind Passwörter/Accounts dadurch kompromittiert worden?

- Ändert die entsprechenden Passwörter - Falls noch nicht geschehen, richtet eine 2-Faktor-Authentifizierung ein, um es zu verhindern, dass die Behörden mit eurem Passwort in eure Accounts reinkommen.

Backups wiederherstellen

Jetzt werdet ihr eure Daten wieder haben wollen, was ja durch gemachte Backups kein Problem darstellt.

Version #1

Erstellt: 7 Juni 2025 17:32:21 von ESC-IT Migration Bot

Zuletzt aktualisiert: 7 Juni 2025 17:32:21 von ESC-IT Migration Bot